CLAIM AMENDMENTS

1. (Cancelled)

2. (Currently Amended) An extremely secure method for a host processor to key a source content to a source storage medium to prevent use of an unauthorized copy of the source content comprising the host processor storing a fingerprinted content comprising the steps of:

the host processor determining a source fingerprint from the source storage medium, wherein the source fingerprint is a physical attribute of the source storage medium;

the host processor combining the source content to be secured with the source fingerprint to generate the fingerprinted content;

the host processor instructing the source storage medium to store the fingerprinted content; and

~~The extremely secure method of Claim 1 further comprising the step of a~~ the host processor reading and verifying the fingerprinted content, including~~the reading and verifying step comprising the steps of~~:

the host processor instructing a local storage medium to read the fingerprinted content;

the host processor separating the source content to be secured from the source fingerprint;

the host processor requesting a local fingerprint from the local storage medium; and

the host processor comparing the local fingerprint with the source fingerprint and in response to the comparison determining whether to use the source content.

3. (Previously Presented) The extremely secure method of Claim 2 wherein the step of the host processor determining a source fingerprint further comprises:

the host processor using an open protocol to request a secured communication from the source storage medium;

the host processor identifying a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic associated with the source storage medium;

generating encryption and/or decryption keys;

returning the encryption key to the host processor;

the host processor using the encryption key to convert the source content to an encrypted protocol;

the host processor requesting from the source storage medium the PSUVI characteristic; and

the source storage medium responding to the host processor with the PSUVI characteristic.

4. (Previously Presented) The extremely secure method of Claim 2 wherein the step of the host processor combining the source content with the source fingerprint to generate the fingerprinted content further comprises:

the host processor creating a hybrid content to be secured by combining the source content to be secured and the source fingerprint; and

the host processor encrypting the fingerprinted content with an encryption key.

5. (Previously Presented) The extremely secure method of Claim 2 wherein the step of the host processor requesting a local fingerprint from the local storage medium further comprises the steps of:

the host processor requesting from the local storage medium a local PSUVI characteristic;

the local storage medium replying to the host processor with the local PSUVI characteristic; and

the host processor performing a secured verification of the local PSUVI characteristic.

6. (Previously Presented) The extremely secure method of Claim 2 wherein the step of the host processor determining a source fingerprint further comprises:

the host processor using an open protocol to request a secured communication from the source storage medium;

the host processor identifying a relatively mutable physical attribute (Non-PSUVI) characteristic associated with the source storage medium;

generating encryption and/or decryption keys;

returning the encryption key to the host processor;

the host processor using the encryption key to convert the source content to an encrypted protocol;

the host processor requesting from the source storage medium the non-PSUVI characteristic; and

the source storage medium responding to the host processor with the non-PSUVI characteristic.

7. (Previously Presented) The extremely secure method of Claim 2 wherein the step of the host processor requesting a local fingerprint from the local storage medium further comprises the steps of:

the host processor requesting from the local storage medium a local non-PSUVI characteristic;

the local storage medium replying to the host processor with the local non-PSUVI characteristic; and

the host processor performing a secured verification of the local non-PSUVI characteristic.

8-21. (Cancelled)

22. (Previously Presented) A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a source fingerprint of a hard disk drive, wherein the source fingerprint is a physical attribute of the hard disk drive;

transferring the source fingerprint from the hard disk drive to the host processor; then

generating a fingerprinted source content in the host processor using the source content and the source fingerprint, wherein the fingerprinted source content represents the source content and the source fingerprint; then

transferring the fingerprinted source content from the host processor to the hard disk drive;

storing the fingerprinted source content in the hard disk drive; then

retransferring the fingerprinted source content from the hard disk drive to the host processor;

generating the source content and the source fingerprint from the retransferred fingerprinted source content in the host processor;

retransferring the source fingerprint from the hard disk drive to the host processor; and then

comparing the generated source fingerprint with the retransferred source fingerprint in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison.

23. (Previously Presented) The method of Claim 22, wherein the source fingerprint is a statistically unique physical attribute of the hard disk drive.

24. (Previously Presented) The method of Claim 23, wherein the source fingerprint is a relatively immutable physical attribute of the hard disk drive.

25. (Previously Presented) The method of Claim 24, wherein the source fingerprint is a statistically unique, immutable and verifiable physical attribute of the hard disk drive.

26. (Previously Presented) The method of Claim 22, wherein the source fingerprint is a defect list of the hard disk drive.

27. (Previously Presented) The method of Claim 26, wherein the defect list includes physical block addresses.

28. (Previously Presented) The method of Claim 22, wherein the source fingerprint is a servo characteristic of the hard disk drive.

29. (Previously Presented) The method of Claim 28, wherein the servo characteristic is servo burst correction values.

30. (Previously Presented) The method of Claim 28, wherein the servo characteristic is servo burst correction value related repeatable runout response.

31. (Previously Presented) The method of Claim 28, wherein the servo characteristic is servo wedge defects.

32. (Previously Presented) The method of Claim 28, wherein the servo characteristic is a servo transfer function.

33. (Previously Presented) The method of Claim 22, wherein the source fingerprint is a track misregistration behavior of the hard disk drive.

34. (Previously Presented) The method of Claim 22, wherein the source fingerprint is a channel optimization of the hard disk drive.

35. (Previously Presented) The method of Claim 34, wherein the channel optimization is a read channel optimization parameter related to an individual head.

36. (Previously Presented) The method of Claim 34, wherein the channel optimization is a write channel optimization parameter related to an individual head.

37. (Previously Presented) The method of Claim 22, wherein the source fingerprint is a statistically unique physical property of a head disk assembly of the hard disk drive.

38. (Previously Presented) The method of Claim 22, wherein the source fingerprint is a statistically unique physical property of a printed circuit board of the hard disk drive.

39. (Previously Presented) The method of Claim 22, wherein the source fingerprint is magnetic defects of the hard disk drive.

40. (Previously Presented) The method of Claim 22, wherein the source fingerprint is a head/media characteristic of the hard disk drive.

41. (Previously Presented) The method of Claim 22, including transferring an encryption key from the hard disk drive to the host processor.

42. (Previously Presented) The method of Claim 41, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the source fingerprint in the host processor.

43. (Previously Presented) The method of Claim 41, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the source fingerprint in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

44. (Previously Presented) The method of Claim 22, wherein generating the fingerprinted source content includes encrypting the source content and the source fingerprint using an encryption algorithm.

45. (Previously Presented) The method of Claim 22, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

46. (Previously Presented) The method of Claim 22, wherein comparing the generated source fingerprint with the retransferred source fingerprint includes determining whether the generated source fingerprint and the retransferred source fingerprint match using statistical analysis.

47. (Previously Presented) The method of Claim 46, wherein the statistical analysis includes determining whether a statistically large percentage of defects listed in the generated source fingerprint point to defects in the retransferred source fingerprint.

48. (Previously Presented) The method of Claim 46, wherein the statistical analysis includes determining whether a statistically small percentage of defects listed in the generated source fingerprint point to defects in the retransferred source fingerprint.

49. (Previously Presented) The method of Claim 22, wherein the generated source content is enabled for use by the host processor if the generated source fingerprint matches the retransferred source fingerprint, and the generated source content is disabled for use by the host processor if the generated source fingerprint does not match the retransferred source fingerprint.

50. (Previously Presented) The method of Claim 22, wherein the host processor uses the generated source content if the generated source fingerprint matches the retransferred source fingerprint, and the host processor does not use the generated source content if the generated source fingerprint does not match the retransferred source fingerprint.

51. (Previously Presented) A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a source fingerprint of a hard disk drive, wherein the source fingerprint is a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic of the hard disk drive;

transferring the source fingerprint from the hard disk drive to the host processor; then

generating a fingerprinted source content in the host processor using the source content and the source fingerprint, wherein the fingerprinted source content represents the source content and the source fingerprint; then

transferring the fingerprinted source content from the host processor to the hard disk drive;

storing the fingerprinted source content in the hard disk drive; then

retransferring the fingerprinted source content from the hard disk drive to the host processor;

generating the source content and the source fingerprint from the retransferred fingerprinted source content in the host processor;

retransferring the source fingerprint from the hard disk drive to the host processor; and then

comparing the generated source fingerprint with the retransferred source fingerprint in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison.

52. (Previously Presented) The method of Claim 51, wherein the source fingerprint is an immutable characteristic of the hard disk drive.

53. (Previously Presented) The method of Claim 51, wherein the source fingerprint is a defect list.

54. (Previously Presented) The method of Claim 51, including transferring an encryption key from the hard disk drive to the host processor.

55. (Previously Presented) The method of Claim 54, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the source fingerprint in the host processor.

56. (Previously Presented) The method of Claim 54, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the source fingerprint in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

57. (Previously Presented) The method of Claim 51, wherein generating the fingerprinted source content includes encrypting the source content and the source fingerprint using an encryption algorithm.

58. (Previously Presented) The method of Claim 51, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

59. (Previously Presented) The method of Claim 51, wherein the generated source content is enabled for use by the host processor if the generated source fingerprint matches the retransferred source fingerprint, and the generated source content is disabled for use by the host processor if the generated source fingerprint does not match the retransferred source fingerprint.

60. (Previously Presented) The method of Claim 51, wherein the host processor uses the generated source content if the generated source fingerprint matches the retransferred source fingerprint, and the host processor does not use the generated source content if the generated source fingerprint does not match the retransferred source fingerprint.

61. (Previously Presented) A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a media defect list of the hard disk drive;

transferring the media defect list from the hard disk drive to the host processor; then

generating a fingerprinted source content in the host processor using the source content and the media defect list, wherein the fingerprinted source content represents the source content and the source fingerprint; then

transferring the fingerprinted source content from the host processor to the hard disk drive;

storing the fingerprinted source content in the hard disk drive; then

retransferring the fingerprinted source content from the hard disk drive to the host processor;

generating the source content and the media defect list from the retransferred fingerprinted source content in the host processor;

retransferring the media defect list from the hard disk drive to the host processor; and then

comparing the generated media defect list with the retransferred media defect list in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison.

62. (Previously Presented) The method of Claim 61, wherein the media defect list is a statistically unique, immutable and verifiable physical attribute of the hard disk drive.

63. (Previously Presented) The method of Claim 61, wherein the media defect list includes physical block addresses.

64. (Previously Presented) The method of Claim 61, including transferring an encryption key from the hard disk drive to the host processor.

65. (Previously Presented) The method of Claim 64, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the media defect list in the host processor.

66. (Previously Presented) The method of Claim 64, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the media defect list in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

67. (Previously Presented) The method of Claim 61, wherein generating the fingerprinted source content includes encrypting the source content and the media defect list using an encryption algorithm.

68. (Previously Presented) The method of Claim 61, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

69. (Previously Presented) The method of Claim 61, wherein the generated source content is enabled for use by the host processor if the generated media defect list matches the retransferred media defect list, and the generated source content is disabled for use by the host processor if the generated media defect list does not match the retransferred media defect list.

70. (Previously Presented) The method of Claim 61, wherein the host processor uses the generated source content if the generated media defect list matches the retransferred media defect list, and the host processor does not use the generated source content if the generated media defect list does not match the retransferred media defect list.

71. (Previously Presented) A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a first source fingerprint of a first hard disk drive, wherein the first source fingerprint is a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic of the first hard disk drive;

providing a second source fingerprint of a second hard disk drive, wherein the second source fingerprint is a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic of the second hard disk drive;

transferring the first source fingerprint from the first hard disk drive to the host processor;

generating a fingerprinted source content in the host processor using the source content and the first source fingerprint, wherein the fingerprinted source content represents the source content and the first source fingerprint; then

transferring the fingerprinted source content from the host processor to a selected hard disk drive;

storing the fingerprinted source content in the selected hard disk drive; then

retransferring the fingerprinted source content from the selected hard disk drive to a host device;

generating the source content and the first source fingerprint from the retransferred fingerprinted source content in the host device;

transferring a selected source fingerprint from the selected hard disk drive to the host device, wherein the selected source fingerprint is the first source fingerprint if the selected hard disk drive is the first hard disk drive, and the selected source fingerprint is the second source fingerprint if the selected hard disk drive is the second hard disk drive; and then

comparing the generated source fingerprint with the selected source fingerprint in the host device, wherein the host device determines that the generated source content is sanctioned if the generated source fingerprint matches the selected source fingerprint, and the host device determines that the generated source content is unsanctioned if the generated source fingerprint does not match the selected source fingerprint.

72. (Previously Presented) The method of Claim 71, wherein the first source fingerprint is an immutable characteristic of the first hard disk drive, and the second source fingerprint is an immutable characteristic of the second hard disk drive.

73. (Previously Presented) The method of Claim 71, wherein the first source fingerprint is a first defect list of the first hard disk drive, and the second source fingerprint is a second defect list of the second hard disk drive.

74. (Previously Presented) The method of Claim 73, wherein the first defect list includes first physical block addresses, and the second defect list includes second physical block addresses.

75. (Previously Presented) The method of Claim 71, wherein the first source fingerprint is a first servo characteristic of the first hard disk drive, and the second source fingerprint is a second servo characteristic of the second hard disk drive.

76. (Previously Presented) The method of Claim 75, wherein the first servo characteristic is first servo burst correction values, and the second servo characteristic is second servo burst correction values.

77. (Previously Presented) The method of Claim 75, wherein the first servo characteristic is first servo burst correction value related repeatable runout response, and the second servo characteristic is second servo burst correction value related repeatable runout response.

78. (Previously Presented) The method of Claim 75, wherein the first servo characteristic is first servo wedge defects, and the second servo characteristic is second servo wedge defects.

79. (Previously Presented) The method of Claim 75, wherein the first servo characteristic is a first servo transfer function, and the second servo characteristic is a second servo transfer function.

80. (Previously Presented) The method of Claim 71, wherein the first source fingerprint is a track misregistration behavior of the first hard disk drive, and the second source fingerprint is a track misregistration behavior of the second hard disk drive.

81. (Previously Presented) The method of Claim 71, wherein the first source fingerprint is a first channel optimization of the first hard disk drive, and the second source fingerprint is a second channel optimization of the second hard disk drive.

82. (Previously Presented) The method of Claim 81, wherein the first channel optimization is a read channel optimization parameter related to a first individual head, and the second channel optimization is a read channel optimization parameter related to a second individual head.

83. (Previously Presented) The method of Claim 81, wherein the first channel optimization is a write channel optimization parameter related to a first individual head, and the second channel optimization is a write channel optimization parameter related to a second individual head.

84. (Previously Presented) The method of Claim 71, wherein the first source fingerprint is a statistically unique physical property of a head disk assembly of the first hard disk drive, and the second source fingerprint is a statistically unique physical property of a head disk assembly of the second hard disk drive.

85. (Previously Presented) The method of Claim 71, wherein the first source fingerprint is a statistically unique physical property of a printed circuit board of the first hard disk drive, and the second source fingerprint is a statistically unique physical property of a printed circuit board of the second hard disk drive.

86. (Previously Presented) The method of Claim 71, wherein the first source fingerprint is magnetic defects of the first hard disk drive, and the second source fingerprint is magnetic defects of the second hard disk drive.

87. (Previously Presented) The method of Claim 71, wherein the first source fingerprint is a head/media characteristic of the first hard disk drive, and the second source fingerprint is a head/media characteristic of the second hard disk drive.

88. (Previously Presented) The method of Claim 71, including transferring an encryption key from the first hard disk drive to the host processor.

89. (Previously Presented) The method of Claim 88, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the first source fingerprint in the host processor.

90. (Previously Presented) The method of Claim 88, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the first source fingerprint in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

91. (Previously Presented) The method of Claim 71, wherein generating the fingerprinted source content includes encrypting the source content and the first source fingerprint using an encryption algorithm.

92. (Previously Presented) The method of Claim 71, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

93. (Previously Presented) The method of Claim 71, wherein the selected hard disk drive is the first hard disk drive, the selected source fingerprint is the first source fingerprint, and the host device determines that the generated source content is sanctioned.

94. (Previously Presented) The method of Claim 93, wherein the host device is the host processor.

95. (Previously Presented) The method of Claim 71, wherein the selected hard disk drive is the second hard disk drive, the selected source fingerprint is the second source fingerprint, and the host device determines that the generated source content is unsanctioned.

96. (Previously Presented) The method of Claim 95, wherein the host device is another processor.

97. (Previously Presented) The method of Claim 95, wherein transferring the fingerprinted source content from the host processor to the second hard disk drive includes transferring the fingerprinted source content from the host processor to the first hard disk drive, and then transferring the fingerprinted source content from the first hard disk drive to the second hard disk drive.

98. (Previously Presented) The method of Claim 97, wherein transferring the fingerprinted source content from the first hard disk drive to the second hard disk drive includes transferring a drive image copy of the fingerprinted source content from the first hard disk drive to the second hard disk drive.

99. (Previously Presented) The method of Claim 97, wherein transferring the fingerprinted source content from the first hard disk drive to the second hard disk drive is performed using low-level block copy software.

100. (Previously Presented) The method of Claim 97, wherein the host device is another processor.

101. (Previously Presented) The method of Claim 71, wherein the host device is the host processor.

102. (Previously Presented) The method of Claim 71, wherein the host device is another processor.

103. (Previously Presented) The method of Claim 71, wherein comparing the generated source fingerprint with the selected source fingerprint includes determining whether the generated source fingerprint and the selected source fingerprint match using statistical analysis.

104. (Previously Presented) The method of Claim 103, wherein the statistical analysis includes determining whether a statistically large percentage of items listed in the generated source fingerprint are consistent with the selected source fingerprint.

105. (Previously Presented) The method of Claim 103, wherein the statistical analysis includes determining whether a statistically small percentage of items listed in the generated source fingerprint are inconsistent with the selected source fingerprint.

106. (Previously Presented) The method of Claim 103, wherein the statistical analysis includes determining whether a statistically large percentage of defects listed in the generated source fingerprint point to defects in the selected source fingerprint.

107. (Previously Presented) The method of Claim 103, wherein the statistical analysis includes determining whether a statistically small percentage of defects listed in the generated source fingerprint point to defects in the selected source fingerprint.

108. (Previously Presented) The method of Claim 71, wherein the generated source content is enabled for use by the host device if the generated source fingerprint matches the selected source fingerprint, and the generated source content is disabled for use by the host device if the generated source fingerprint does not match the selected source fingerprint.

109. (Previously Presented) The method of Claim 71, wherein the host device uses the generated source content if the generated source fingerprint matches the selected source fingerprint, and the host device does not use the generated source content if the generated source fingerprint does not match the selected source fingerprint.

110. (Previously Presented) The method of Claim 71, wherein the host device determines that the generated source content is an authorized copy of the source content if the generated source fingerprint matches the selected source fingerprint, and the host device determines that the generated source content is an unauthorized copy of the source content if the generated source fingerprint does not match the selected source fingerprint.